UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/666,140	09/20/2000	Joseph G. Barrett	06975-131001	5787

26171   7590   11/28/2007

FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER
NGUYEN, VAN KIM T

ART UNIT	PAPER NUMBER
2152	

MAIL DATE	DELIVERY MODE
11/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	09/666,140	BARRETT ET AL.
	Examiner	Art Unit	
	Van Kim T. Nguyen	2152	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>04 September 2007</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,4 and 6-45* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,4 and 6-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   This Office Action is responsive to communications filed on September 4, 2007.

Claim 2 is cancelled, 38-45 are added, thus claims 1, 3-4, and 6-45 are pending in the case.

Response to Arguments

2.   Applicant's arguments filed September 4, 2007 have been fully considered but

they are not persuasive.

In response to applicant's arguments against the references individually, one cannot show

nonobviousness by attacking references individually where the rejections are based on

combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re*

Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, Eichstaedt teaches

substantially all the claimed limitations, i.e., monitoring a computer for connection transactions

between multiple requestors and access provider using a switching component connected to the

access provider and denying access by attacking requestor to the access providers when a

number of connection transaction initiated by the attacking access requestor through the

switching component exceeds a configurable threshold. However, Eichstaedt does not explicitly

call for multiple access providers. Short teaches connections between multiple access requestors

and multiple access providers, thus it meets the claims.

Claim Rejections - 35 USC § 103

3.   The text of those sections of Title 35, U.S. Code not included in this action can be

found in a prior Office action.

4.   Claims 1-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Eichstaedt et al. (U.S. Patent No. 6,662,230), hereinafter Eichstaedt, in view of Short et al.(US

6,636,894), hereinafter Short.

Regarding claims 1, 8-9, 13, 15, 23, 25, 34, 38-39 and 45, as shown in Figures 1-6,

Eichstaedt discloses:

monitoring a computer system for connection transactions between multiple requestors

(12, 14, 16) and an access provider (21) using a switching component (22, 11) connected to the

access provider (col. 5: lines 32-39; and col. 11: lines 62-67);

denying access by an attacking access requestor (16) to the access provider (21) when a

number of connection transactions initiated by the attacking access requestor (e.g., request

values) through the switching component (11) exceeds a configurable threshold number (e.g.,

maximum request values) during a first configurable period of time (col. 6: lines 43-61; and col.

12: lines 3-20).

Eichstaedt also discloses the monitoring includes detecting connection transactions

between multiple Internet protocol addresses and the access provider with the switching

components (Eichstaedt; col. 5: lines 32-39; and col. 7: lines 23-49).

Eichstaedt does not explicitly call for a plurality of access providers.

As shown in Figure 1, Short teaches a system and method for providing multiple users

(14) access to a plurality of networks (22 and 20), see col. 6: line 9 – col. 7: line 24.

It would have been obvious to one of ordinary skill in the art at the time the invention

was made to apply Short's method of providing multiple users access to a plurality of network

providers in Eichstaedt's system, motivated by the need of providing users access to the Internet,

i.e., a worldwide, publicly accessible network of interconnected computer networks that transmit

data, consisting of millions of smaller domestic, academic, business, and government networks.

Regarding claim 3, Eichstaedt-Short also discloses the monitoring further includes

counting, using the switching component, and comparing the number of connection transactions

initiated by the access requestors to any of the access providers (e.g., request values) through the

switching component (e.g., 22, 11) during the first configurable period of time (t_1) to the

configurable threshold (e.g., a comparison between the calculated request values and a

predefined maximum value is made; Eichstaedt; col. 7: lines 5-10 and lines 21-49).

Regarding claims 4, 16 and 26, Eichstaedt-Short also discloses:

the monitoring further includes comparing, using the switching component, the number

of connection transactions initiated by the access requestors through the switching component

during the first configurable period of time to the configurable threshold number (e.g., a

comparison between the calculated request values and a predefined maximum value is made

during t_1; Eichstaedt; col. 7: lines 5-10 and lines 21-49), and

denying access by the attacking access requestor to the access providers includes

denying, using the switching component, access by the attacking access requestor to all of the

access providers connected to the switching component when the comparison results indicate

that the number of connection transactions initiated by the attacking access requestor during the

first configurable period of time exceeds the configurable threshold number (e.g., denying access

after failing cumulative data check; Eichstaedt, col.: lines 3-20).

Regarding claim 6, Eichstaedt-Short also discloses the monitoring further includes

counting, using the switching component, the number of connection transactions initiated to any

of the access providers by the Internet protocol addresses during the first configurable period of

time such that the number of connection transactions reflects a cumulative number of connection

transactions initiated to any of the access providers by the Internet protocol addresses (step 86,

Figure 4; col. 8: line 56 – col. 9: line 15).

Regarding claims 7, 17 and 27, Eichstaedt-Short also discloses the monitoring further

includes

comparing, using the switching component, the number of connection transactions

initiated by the internet protocol addresses during the first configurable period of time to the

configurable threshold number (e.g., a comparison between the calculated request values and a

predefined maximum value is made during first frequency t_1; Eichstaedt; col. 7: lines 5-10 and

lines 21-49), and

denying access by the attacking access requester to the access providers includes

denying, using the switching component, access by the attacking access requestor to all of the

access providers connected to the switching component when the comparison results indicate

that the number of connection transactions initiated by the Internet protocol address associated

with the attacking access requestor during the first configurable period of time exceeds the

configurable threshold number (step 86, Eichstaedt; Figure 4; col. 8: line 56 – col. 9: line 15).

Regarding claims 10-12, 20-22, and 30-33, Eichstaedt-Short discloses that the denying of access includes denying access to the access providers through the switching component (e.g., 22, 11) by the attacking access requestor (e.g., 16) for a second configurable period of time (t_i) after detecting a most recent connection transaction initiated by the attacking requestor through the switching component (Eichstaedt; col. 4: lines 12-17; and col. 7: lines 31-49).

Regarding claims 36, Eichstaedt-Short also discloses a host computer system (e.g., 21) receives communication from the switching component (e.g., 22, 11), see Eichstaedt, Figure 1.

Regarding claims 37, Eichstaedt-Short also discloses the switching system (e.g., 22, 11) is included in a host system (e.g., 21), see Eichstaedt, Figure 1.

5.   Claims 40-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Eichstaedt, in view of Short, as applied to claim 39 above, and further in view of Lin et al (US 6,751,668).

Regarding claim 40, Eichstaedt-Short discloses substantially all the claimed limitations, except the establishment of a communication link between the attacking access requestor and one of the access providers involving exchange of more than two electronic messages.

Lin discloses establishment of a communication link between the attacking access requestor and one of the access providers involving exchange of more than two electronic messages (e.g., SYN and SYN/ACK; Figure 1, col. 2: lines 2-9).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize Lin's method of responding to service attacks in Eichstaedt-Short's system in order to limiting unwanted access to server data.

Regarding claim 41, Eichstaedt-Short-Lin also discloses:

determining, using the switching component, that the second configurable time period, has passed without detecting a new connection transaction initiated by the attacking access requestor to any of the access providers through the switching component (e.g., monitoring the rate of receipt of session establishment; Figure 2: lines 30-43); and

in response to determining at the second configurable time period has passed without detecting a new connection transaction initiated by the attacking access requestor to any of the access providers through the switching component, allowing access by an attacking access requestor to the access providers (e.g., monitoring the rate of receipt of session establishment is less that the MAX_SESS_RATE, the state machine moves back to the normal state 202; Figure 2: lines 30-43).

6.   Claims 42-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Eichstaedt, in view of Short, as applied to claim 1 above, and further in view of Joiner (US 6,742,128).

Regarding claim 42, Eichstaedt-Short also discloses:

the access providers include a first access provider and a second access provider that is different from the first access provider (e.g., computer network 20 and online services 22; Short, Figure 1; col. 6: lines 46-67);

Eichstaedt-Short also discloses monitoring for connection transactions between multiple access requestors and access providers using the switching component connected to the access providers (Eichstaedt; col. 5: lines 32-39; and col. 11: lines 62-67 and Short; Figure 1), it would have been obvious to one of ordinary skill in the art at the time the invention was made Eichstaedt-Short can be used to detecting, using the switching component, for detecting the number of connection transaction at each of the access providers;

Eichstaedt-Short also discloses denying access by the attacking access requestor to the access provider when the number of connection transaction initiated by the attacking access requestor through the switching component exceeds the configurable threshold number during the first configurable period (step 86, Eichstaedt; Figure 4; col. 8: line 56 – col. 9: line 15).

However, Eichstaedt-Short does not explicitly call for denying access when a sum of the first number of connection transactions and the second number of connection transactions exceeds the configurable threshold number.

As shown in Figures 1-8, Joiner teaches collecting network data from a plurality of network data source and the various network data may be aggregated and correlated for enhancing threshold-based alert (col. 6: line 65 – col. 7: line 63, col. 9: lines 19-45; and col. 10: lines 41-60).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Joiner's method of assessing threat in Eichstaedt-Short's system in order to improve the network security by provide protection against denial of service attacks.

Regarding claim 43, Eichstaedt-Short-Joiner also discloses:

detecting, using the switching component, the first number of connection transactions initiated by the attacking access requestor to the first access provider during the first configurable period of time includes detecting a first number of connection transactions that exceeds the configurable threshold number during the first configurable period of time (Eichstaedt; col. 5: lines 32-39, col. 8: line 56 – col. 9: line 15, and col. 11: lines 62-67 and Short; Figure 1);

detecting, using the switching component, a second number of connection transactions initiated by the attacking access requestor to the second access provider during the first, configurable period of time includes detecting zero connection transactions initiated by, the attacking access requestor the second access provider during the first configurable period of time (Eichstaedt; col. 5: lines 32-39, col. 8: line 56 – col. 9: line 15, and col. 11: lines 62-67 and Short; Figure 1); and

denying access by the attacking access requestor to both the first access provider and the second access provider when a sum of the first number of connection transactions and the second number of connection transactions exceeds the configurable threshold number includes denying access by the attacking access requestor to both the first access provider and the second access provider when the first number of connection transactions exceeds the configurable threshold number and the second number of connection transactions is zero (Joiner; col. 6: line 65 – col. 7: line 63, col. 9: lines 19-45; and col. 10: lines 41-60).

Regarding claim 44, Eichstaedt-Short also discloses:

detecting, using the switching component, the first number of connection transactions initiated lay the attacking access requestor to the first access provider during the first

configurable period of time includes detecting a first number of connection transactions that is

less than the configurable threshold number during the first configurable period of time

(Eichstaedt; col. 5: lines 32-39, col. 8: line 56 – col. 9: line 15, and col. 11: lines 62-67 and

Short; Figure 1),

detecting, using the switching component, a second number of connection transactions

initiated by the attacking access requestor to the second access provider during the first

configurable period of time includes (Eichstaedt; col. 5: lines 32-39, col. 8: line 56 – col. 9: line

15, and col. 11: lines 62-67 and Short; Figure 1);

detecting a second number of connection transactions that is less than the configurable

threshold number during the first configurable period of time, the sum of the first number of

connection transactions and the second number of connection transactions exceeding the

configurable threshold number (Eichstaedt; col. 5: lines 32-39, col. 8: line 56 – col. 9: line 15,

and col. 11: lines 62-67 and Short; Figure 1); and

denying access by the attacking access requestor to both the first access provider and the

second, access provider when a sum of the first number of connection transactions and the

second number of connection transactions exceeds the configurable threshold number includes

denying access by the attacking access requestor to both the first access provider and the second

access provider when the sum of the first number of connection transactions and the second

number of connection transactions exceeds the configurable threshold number, even though

neither the first number of connection transactions nor the second number of connection

transactions exceeds the configurable threshold number (Joiner; col. 6: line 65 – col. 7: line 63,

col. 9: lines 19-45; and col. 10: lines 41-60).

Conclusion

7.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of

time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

8.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Van Kim T. Nguyen whose telephone number is 571-272-3073.

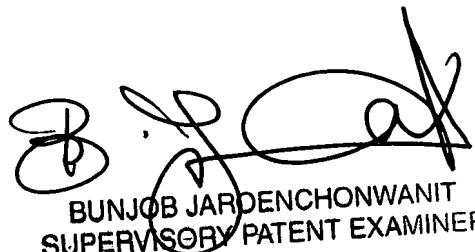The examiner can normally be reached on 8:00 AM - 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Bunjob Jaroenchonwanit can be reached on 571-272-3913. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Van Kim T. Nguyen
Examiner
Art Unit 2152

vkn

BUNJOB JARDENCHONWANIT
SUPERVISORY PATENT EXAMINER
11/26/7